The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems

scripted

Volume 6, Issue 1, April 2009

The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822

Wiebke Abel and Burkhard Schafer**

Abstract

On the 27th of February 2008, the German Federal Constitutional Court (Bundesverfassungsgericht) recognised in a landmark ruling for the first time a new constitutional right in the confidentiality and integrity of information technology systems. We will show in this case commentary why the Court found it necessary to introduce new legislation, and provide an overview of the newly established constitutional right.

DOI: 10.2966/scrip.060109.106

* Research Associate, SCRIPT; PhD Candidate in Law, University of Edinburgh; LLM, University of Edinburgh (2006).

* Senior Lecturer, University of Edinburgh, School of Law.

1. Introduction

On the 27th of February 2008, the German Federal Constitutional Court (Bundesverfassungsgericht)[1] recognised in a landmark ruling for the first time a new constitutional right in the confidentiality and integrity of information technology systems.[2] The primary question the Court had to decide was the constitutionality of a law authorising the secret services of North Rhine-Westphalia to surreptitiously monitor and investigate the Internet. In particular, the law would have granted the secret services the right to clandestinely intercept and search for communication via the Internet, and to secretly access its information technology systems. This law had been introduced as an amendment to Art 5.2 no. 11 of the Act on the Protection of the Constitution in North Rhine-Westphalia (Gesetz über den Verfassungsschutz in Nordrhein-Westfalen) from 20 December 2006.

The Court held in its judgement that such investigative actions do indeed interfere with constitutionally guaranteed rights. Any legislation permitting such actions therefore must be able to demonstrate that such an interference is justified by the protection of other constitutional rights, necessary to achieve this protection and proportionate in its impact. The Court found that the legislation as drafted was not in accordance with the Constitution, and therefore unlawful.[3]

It had been widely anticipated that the Court would rule the amendment unconstitutional.[4] The preliminary hearing before the Constitutional Court had also suggested this outcome.[5] However, the reasoning of the Court and the scope of the decision came as a surprise to most observers. Most had expected that the Court would merely extend its comprehensive jurisprudence on search and seizure requirements for physical premises to the online environment. Instead, the Court created in its decision a new fundamental right, which explicitly protects privacy and personality rights of citizens in information and communication technology (ICT).

2. Background of the Case

The subject of the decision was the amendment of § 5.2 of the Act on the Protection of the Constitution in North Rhine-Westphalia from 20 December 2006. However, the amendment of this law was only one aspect in a discussion at federal level about the legality of a new type of investigation methods, the remote searching of computers and laptops. It is therefore necessary to give an account of this preceding debate.

The public and legal debate on this subject was triggered in 2006 by the application of a state prosecutor to the German Federal Court of Justice (Bundesgerichtshof, BGH).

---

[1] Hereafter "the Court".

[2] BVerfG, NJW 2008, 822.

[3] Ibid.

[4] See e.g. G Hornung, " Ein neues Grundrecht. Der verfassungsrechtliche Schutz der "Vertraulichkeit und Integrität informationstechnischer Systeme"", (2008) 5 *Computer und Recht*, 299.

[5] M Kutscha, "Mehr Schutz von Computerdaten durch ein neues Grundrecht?", (2008) 15 *Neue Juristische Wochenschrift*, 1042-1044.

In this application, he asked for a warrant to search remotely a suspect's computer in a terrorism investigation, by covertly installing a surveillance programme similar to a Trojan. The application was rejected on the 25 November 2006. The state prosecutor appealed, claiming that Articles 102[6], 110[7] and 94[8] of the Criminal Code (Strafprozessordnung- StPO) allowed for such a search. His argument assumed a substantial similarity between the physical search of premises, regulated in these articles, and the remote access of a suspect's computer. The BGH disagreed, rejecting in its judgement the analogy between a traditional search of physical premises and clandestine searches of a computer.[9] However, the decision mainly addressed formal procedural questions, ruling that without explicit legislation, granting such a warrant request would be ultra vires. The ruling left open the possibility that appropriate legislation could be introduced to create such new search and seizure powers, and it avoided any substantive decision as to the potential conflict such a law could create with fundamental constitutional guarantees. The State of North Rhine-Westphalia, by amending its existing law for the protection of the constitution, created just such a legal power.

The Act on the Protection of the Constitution in North Rhine-Westphalia outlines the rights of, and establishes a legal basis for operations by, the Constitution Protection Agency, Germany's main secret service for internal affairs. Article 5.2 of this Act defines permissible actions to acquire information and private data from suspects. The amendment in question, of Article 5.2(11) of the North Rhine-Westphalia Constitution Protection Act, empowered the Constitution Protection Agency to carry out two types of investigative measures: Firstly, secret monitoring and other reconnaissance of the Internet (alternative 1), and secondly secret access to information technology systems (alternative 2). Secret monitoring of the Internet is a measure by which the Constitution Protection Agency obtains information about the content of Internet communication using the communication technology in the way it was intended to be used. These can be measures such as accessing an open website, participation in chats or online fora, but also accessing an email inbox or accessing restricted websites using a password obtained elsewhere, for example from an informant.[10] By contrast, the secret access to an information technology system is understood to be its technical infiltration, by taking advantage of the security loopholes of the target system, or by installing a spy program.[11]

The method at the core of the decision, infiltration of a computer through technical means, also referred to as "online search", "Federal Trojan", or "remote searching", is one specific form of such information gathering. This investigative method tries to accommodate the difficulties in investigations that emerge if criminal offenders, in

---

[6] Regulates the search of premises.

[7] Regulates the seizure and search of documents and digital storage devices.

[8] Regulates the securing and seizure of evidence.

[9] BGH, NJW 2007, 930.

[10] BVerfG, NJW 2008, 822 (825).

[11] Ibid.

particular those from extremist and terrorist groups, use the Internet for communication and to plan and commit criminal offences.[12]

The purpose of remotely searching a computer is to enable investigators to search the data stored on the hard disk and the working memory of the computer, to intercept the email traffic, and monitor web browsing habits and instant messaging.[13] To accomplish this, a specifically designed computer program, a "remote forensic software" (RFS) tool, is planted on the suspect's computer without his knowledge. This program is then able to copy all data stored on the computer and subsequently transfer it back to the investigating authority for evaluation. Such a program shares crucial features with well-known malware, in particular viruses and Trojans.[14] The latter in particular can be used to access and extract personal data from targets, and hence is equally suitable for data collection by police authorities. This is why the RFS tool facilitating remote searches is often referred to as a "Federal Trojan" in Germany. The advantage of using these technologies is that they can be installed clandestinely, and without access to the suspect's house or physical premises. They are designed to be disguised as something harmless, when they actually include malicious or harmful code, and therefore trick the suspect into installing them. Therefore, as with their criminal counterparts, police Trojans require the unwitting cooperation of the target.[15] This can happen through opening an email, for instance an email that purports to come from a bona fide state agency such as the local council or the Department for Pensions.

If the infiltration is successful this method offers considerable advantages to the investigation authority in comparison to traditional investigation methods. Because the method is undertaken without the knowledge of the suspect, this person is not alerted to the fact that the police considers him a target, as opposed to a traditional house search. Furthermore, it allows collecting encrypted data in an unencrypted form as the investigating authority can access the data while the user is typing it. Moreover, passwords and further information on the usage pattern of the suspect can be collected. This kind of information would hardly ever be possible to obtain using traditional investigation methods.[16]

A constitutional complaint is only admissible under German law if the complainant can show that he is directly affected by the state act, and that one of the fundamental rights enumerated in the first part of the Constitution is violated. The amendment of § 5.2 of the Act on the Protection of the Constitution in North Rhine-Westphalia limits the applicability of this norm to illegal activities "*threatening the free democratic fundamental order or the continued existence or the security of the Federation or of a Federal state"*[17]*,* and during the discussion about the introduction of the online search as an investigative measure at federal level it was established that this should only be

---

[12] BVerfG, NJW 2008, 822 (826).

[13] K Leipold, "Die Online-Durchsuchung", (2007) 4 *Neue Juristische Wochenschrift Spezial* 135.

[14] U Buermeyer, "Die 'Online-Durchsuchung' – Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme", (2007) 4 *Höchstrichterliche Rechtsprechung im Strafrecht* 154.

[15] Ibid.

[16] BVerfG, NJW 2008, 822 (826).

[17] § 3.1 Verfassungsschutzgesetz Nordrhein-Westfalen.

used to investigate suspects in terrorist investigations or comparably severe cases. Nevertheless, the four claimants filing a constitutional complaint against the amendment of § 5.2 of the Act on the Protection of the Constitution in North Rhine-Westphalia claimed that this law constituted a direct violation of their constitutional rights, even though none of them had been suspects in a criminal investigation. The Court accepted this view and admitted the constitutional complaints. The four claimants could all show that, although not involved in any illegal behaviour themselves, their professional activity might wrongly be classified as such and may cause the remote searching of their computers under the new amendment, thereby violating their rights guaranteed by the constitution. One claimant was a journalist accessing Internet sites operated by persons with extremist views and connections to extremist organisations, and participating in chats hosted on these websites, while also using the computer for private purposes. Another claimant was a member of a political party under observation by the North Rhine-Westphalian Constitution Protection Authority, who was using the computer for both work and private purposes. A further claimant was a lawyer assisting asylum-seekers, some of whom are under observation by the North Rhine-Westphalian constitution protection authority, while using the computer for work and private purposes.

Having passed the first formal hurdle and having been accepted for a substantive decision, the Court now had to determine whether (a) § 5.2 of the Act on the Protection of the Constitution in North Rhine-Westphalia was constitutional, and (b) was invited to consider more generally the constitutionality of this type of investigative methods.

3. The Decision

The Court ruled that § 5.2 of the Act on the Protection of the Constitution in North Rhine-Westphalia was not in compliance with the constitution and therefore null and void. As indicated above, this result did not come as a surprise. However, the expectation had been that the Court would only need to apply the explicitly enumerated basic rights and constitutional principles to reach this conclusion. The Court however found that for several reasons the existing rights canon was not sufficient to protect the constitutional rights of citizens from the potential loss of liberty that the remote searching of computers could cause, and thus created – or maybe inferred from first principles – a new basic right in the confidentiality and integrity of information technology systems.

This surprise move was partly due to the welcome fact that the court engaged in considerable depth with the specific technological issues that the legislation raised. Three of the countries leading academics in the field, Prof Felix Freiling, Chair of Computer Science at the University Mannheim, Prof. Dr. Andreas Pfitzmann, head of the privacy and security group at Dresden University of Technology and Prof. Dr. Dr. hc Ulrich Sieber, director at the Max Planck Institute for Foreign and International Criminal Law were appointed by the court as technical experts. Maybe more unusual was the background of a fourth expert advising the court. Andreas Bogk is a freelance Hacker at Clozure Inc and CEO at Chaos Computer Club Events, one of the biggest and most influential hacker organizations. Their academic and practical expertise was fully matched by the court, whose judges with only one exception all were previous holders of senior academic positions.

3.1 The Respondents

The *Land* (regional) Government of North Rhine-Westphalia (having introduced the new investigative power) and the Federal Government (as a discussant to the Court on this matter, anticipating a similar issue arising in the future for the federal agencies) accepted from the beginning that strict constitutional scrutiny of the new measure was necessary. However, they also argued that RFS tools were sufficiently similar to existing police powers in the offline world that analogous application of the relevant constitutional norms was sufficient. The Land submitted in addition that its law as drafted was compliant with the relevant provision from the constitution. Despite this united front on the principle, the two respondents identified different constitutional norms as "closest off-line match". The Land Government identified the constitutional right guaranteeing the privacy of telecommunications in Article 10.1 of the German Basic Law (Gundgesetz – GG) as applicable law. It argued that remote online search was essentially a new form of wiretapping, and its proposed legislation extended the safeguards in place for wiretapping operations to the new technology. The Federal Government by contrast argued that such investigative measures would best be covered by the fundamental guarantee to the inviolability of the home in Article 13 GG, seeing the online search as the equivalent to the physical search of a suspect's home.

While there was disagreement about the appropriate legal classification of the process of remote online searches, both parties were in agreement regarding the regulation of the outcome of such a search. They conceded that the right to informational self-determination as derived from Article 2.1 GG in connection with Article 1.1 GG could serve as a standard for an online search. The legal argument mirrored in this respect an earlier landmark decision of the Constitutional Court that had shaped Germany's data protection law in the past.

From the position of the state and the investigative authorities, this strategy made sense. They could have argued that the new technology was so different from existing police powers that none of the constitutional norms applied, and only non constitutional law such as criminal law provisions against hacking needed amendment. However, this would have been a high risk strategy with little chance of success. Too obvious was the highly intrusive nature of the remote forensic software (RFS) technology, and too obvious its similarities to constitutionally sensitive forms of surveillance to even attempt to treat it as a mere police procedural issue. By conceding the main point, the state was able to choose its battlefield and design the relevant legislation in such a way that the demands of constitutional compliance did not disrupt police efficiency. The consequences of both articles for police procedure and investigative practice are well understood, and a considerable case law creates a high degree of legal certainty. Since violation of the constitution can result in the inadmissibility of otherwise reliable evidence, this degree of certainty is highly desirable for police practice. A more cynical view would be that over the last decades, police and secret services have learned how to abide by the spirit of these provisions, while working creatively around the restrictions. The codes regulating police procedure and criminal investigation, most importantly the Criminal Procedure Act (Strafprozessordnung StPO) provides the necessary procedure and safeguards that concretise the protective norms of the constitution. The procedural hurdles and requirements that the police have to observe, for instance the warrant requirements, differ in detail between wiretapping and search of premises. Why Federal and State

Government expressed different preferences is not obvious. Broadly speaking, the position of the Regional Government was more aggressive, the position of the Federal Government more restrained, since the protection against physical searches is generally more rigorous than that of wiretapping operations. Conceptually, the two approaches betray a different understanding of the nature of the Internet. The Land took a conservative approach that reduces the experience of the Internet to what it technically is, telecommunication similar to making a phone call. The Federal Government by contrast indicated a willingness to take the user experience and the user understanding of information systems serious, and conceptualised at least certain forms of computer and Internet use not just as an essentially trivial activity rooted in the physical world, but as creating its own, digital world that deserves being taken seriously. Our "home" is partly online, and therefore rules protecting our physical homes should also apply to our digital habitats.

In the next section, we will analyse how the Court responded to these submissions.

3.2 Article 10.1 Grundgesetz – The Secrecy of Telecommunications

The right to the secrecy of telecommunications according to Article 10.1 GG protects the non-physical transmission of information to individual recipients with the aid of telecommunications devices:[18]

> *(1) The privacy of correspondence, posts and telecommunications shall be inviolable.*
>
> *(2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature.*

The protection of this fundamental right covers any type of telecommunication regardless of the transmission type used (cable or broadcast, analogue or digital transmission), and the data transmitted (speech, picture, sound, or other data). The scope of protection of the secrecy of telecommunications therefore also includes any communication via the internet.[19] Furthermore, protected by this right are not only the contents of the communication, but also details about their general circumstances, such as details about the communication partners, and the transmission type (by email, chat, VoIP).[20] Particularly important for online contexts, metadata generated as a result of communication had been included into the scope of the article by the courts in previous decisions. The Court therefore affirmed that any ongoing communication via the internet, and the data generated by such communication falls within the scope of the protection of Article 10.1 GG. Hence, every investigation method targeting

---

[18] See e.g. BVerfGE 67, 157 (172); 106, 28 (35).

[19] See BVerfGE 113, 348 (383) for emails.

[20] See e.g. BVerfGE 67, 157 (172); 85, 386 (396).

ongoing communication and the data related to it has to be in compliance with the right to the secrecy of telecommunications as laid down in Article 10.1 GG. The scope of protection of this fundamental right is affected regardless of whether the measure targets the transmission channel or the terminal used for telecommunication.[21]

As seen above, Art 10(2) GG permits the interception of communication under certain conditions, and the Land Government of North Rhine-Westphalia stated that the amendment of § 5.2 of the Act on the Protection of the Constitution in North Rhine-Westphalia meets the constitutional requirements as to the justification of the encroachment.[22] Procedurally, a law is required that creates the relevant police powers. Substantially, any law that violates prima facie a constitutional right has to have as its aim the protection of another right listed in the constitution, the violation of the right has to be necessary to achieve the intended goal and the violation must be proportionate to protection that is gained.[23] How the legislation achieves this balancing act is however largely left to Parliament. Having for instance a requirement for judicial warrants in such legislation will help it to pass the constitutionality test, but is not a direct constitutional requirement. Conceptualising online surveillance through Trojans as interception of communication was the view proposed by the North Rhine-Westphalian Government and the police forces, based on the notion that the Trojan itself can only function when there is an active communication connection, that is when the computer is connected to the internet and data is transmitted. .

The Court only agreed in parts with this analysis. It found in particular that Article 10.1 GG does not protect telecommunication data that is stored on ICT devices after the communication process is completed, especially if the data is not in the public domain and the affected person has undertaken steps to protect the data from unauthorised access.[24] Furthermore, the Court stated that the protection of Article 10.1 GG does equally not apply if a state agency monitors the use of an information technology system as such, or searches the storage media of the system. This is also the case if a telecommunication connection is used for transmission of the data collected to the evaluating authority, as is the case for instance with searching of computers online.[25] In our opinion, this analysis is correct. That the Trojan requires that the suspect is at some point online and engaged in communication does not make the search a wiretapping operation any more than a police officer who seizes a suspects phone during a physical search of his premises changes the nature of the operation from a search into an interception of telecommunication.

The secret infiltration of a complex information technology system offers the opportunity to spy on the system as a whole, and is not just an intercept of an isolated exchange of communication as in a traditional wiretapping operation.[26] In particular,

---

[21] BVerfGE 106, 28 (37-38); 107, 299 (312-313).

[22] BVerfG, NJW 2008, 822 (841).

[23] BVerfGE 35, 202 "Lebach decision".

[24] BVerfG, NJW 2008, 822 (842).

[25] J Rux, "Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden", (2007) 62 (6) *JuristenZeitung*, 285.

[26] BVerG, NJW 2008, 822 (842).

there is a chance that personal data stored on the computer, which is unrelated to and goes over and above the contents and circumstances of the ongoing telecommunication, is collected (even if this is unintended). Thus, the potential threat to civil liberties goes far beyond the mere surveillance of telecommunication, and also beyond the protective scope of Article 10.1 GG.

The Court therefore came to the conclusion that Article 10.1 GG can only provide sufficient protection against the infiltration of an information technology system if the surveillance is restricted exclusively to data emanating from an ongoing telecommunication process.[27] If the infiltration serves to collect data over and above telecommunications, e.g. by copying data from the hard drive, Article 10.1 GG is not on point. In practice, this means that hardly any search will be a "pure" communications intercept. The main aim of the RFS tool as discussed above is to collect data stored on a computer, and the conceptual gap to communication interception is too wide to be bridged by analogous interpretation of Article 10.1. This also means that several aspects of the remote searching of computers are not covered by the guarantee of secrecy in telecommunications as provided by Article 10.1GG.

3.3 Article 13.1 Grundgesetz – The Inviolability of the Home

The guarantee of the inviolability of the home granted by Article 13.1 GG protects the private living space from intrusion by the state:

> *(1) The home is inviolable.*

This guarantees an essential space to the individual as a necessary precondition for personal dignity, as well as in the interest of the development of ones personality. This guarantee may only be encroached upon under special preconditions as outlined in Article 13.2 to 13.7 GG:

> *2) Searches may be authorized only by a judge or, when time is of the essence, by other authorities designated by the laws, and may be carried out only in the manner therein prescribed.*
>
> *(3) If particular facts justify the suspicion that any person has committed an especially serious crime specifically defined by a law, technical means of acoustical surveillance of any home in which the suspect is supposedly staying may be employed pursuant to judicial order for the purpose of prosecuting the offense, provided that alternative methods of investigating the matter would be disproportionately difficult or unproductive. The authorization shall be for a limited time. The order shall be issued by a panel composed of three judges. When time is of the essence, it may also be issued by a single judge.*
>
> *(4) To avert acute dangers to public safety, especially dangers to life or to the public, technical means of surveillance of the home*

[27] However, this is technically currently still impossible to ensure (See note 4, at 299).

> *may be employed only pursuant to judicial order. When time is of the essence, such measures may also be ordered by other authorities designated by a law; a judicial decision shall subsequently be obtained without delay.*
>
> *(5) If technical means are contemplated solely for the protection of persons officially deployed in a home, the measure may be ordered by an authority designated by a law. The information thereby obtained may be otherwise used only for purposes of criminal prosecution or to avert danger and only if the legality of the measure has been previously determined by a judge; when time is of the essence, a judicial decision shall subsequently be obtained without delay.*
>
> *(6) The Federal Government shall report to the Bundestag annually as to the employment of technical means pursuant to paragraph (3) and, within the jurisdiction of the Federation, pursuant to paragraph (4) and, insofar as judicial approval is required, pursuant to paragraph (5) of this Article. A panel elected by the Bundestag shall exercise parliamentary control on the basis of this report. A comparable parliamentary control shall be afforded by the Länder.*
>
> *(7) Interferences and restrictions shall otherwise only be permissible to avert a danger to the public or to the life of an individual, or, pursuant to a law, to confront an acute danger to public safety and order, in particular to relieve a housing shortage, to combat the danger of an epidemic, or to protect young persons at risk.*

The spatial sphere in which private life takes place constitutes the interests protected by this fundamental right.[28] The private living space is, however, not limited to the private flat or house of the rights holder, but also includes business and office space.[29] It protects this space from physical intrusion, as well as from the use of technical measures that provide an insight into the otherwise protected happenings inside the private living space. This is, for example, the acoustic and optical surveillance of a living space,[30] but also the measurement of electromagnetic radiation to monitor the use of information technology systems inside the dwelling.

The Federal Government argued that the online search of computers can be compared to the search of a house, and Article 13 GG can therefore be used as a standard for such measures. As we have seen, unlike the previous provision, Article 13 contains directly and explicitly non-negotiable conditions for any prima facie infringement. This means that the state is considerably more limited in adjusting the relevant procedural law to accommodate the new technology. While there is no formal ranking

---

[28] See BVerfGE 89, 1 (12); 103, 142 (150-151).

[29] BVerfGE 32, 54 (69).

[30] BVerfGE 109, 279 (309, 327).

between different constitutional rights, the greater care that the drafters used to specify in some details the non-negotiable core of Article 13 in comparison to Article 10 indicates just how serious any interference with the physical space is considered. Consequently, the Federal Government conceded that the high ”intensity” of the encroachment on civil liberties that any restriction of Article 13 brings also means that such a measure should only ever be the ultima ratio for a (federal or state) Constitution Protection Agency.

As with its analysis of Article 10, the Court agreed in parts and rejected the analysis in parts. It found that Article 13.1 GG could only provide protection of the private living space against the secret intrusion by police or secret service to physically manipulate information technology systems, and against the infiltration of such systems to monitor the events in a flat using peripherals connected to the system (such as the use of inbuilt microphones for eavesdropping).[31]

It stated that such actions would be comparable in its nature to the traditional search of a house and would therefore be covered by Article 13 GG. However, even this protection did not go far enough, and it underestimates the importance of the digital world for today’s citizens. The Court argued that Article 13 GG is insufficient to protect rights holders against the general infiltration of information technology systems using a Trojan or similar software to access the stored data and monitor the communication, even if the system is located in a dwelling.[32] One specific problem created by RFS searches is that infiltration and monitoring can be performed regardless of the location of the information technology system. Hence, a location-dependent protection is useless if the system is located outside the private space, or on the move between “protected” areas. Especially small information technology devices such as laptops, PDAs and mobile phones are designed to be carried around. The precise location of the system will often even be unknown, and is also irrelevant for investigators when infiltrating the device to access stored data. This would have had the counterintuitive consequence that a citizen who starts writing an email on his laptop at home, reviews it on a park bench and completes and sends it back at home moves between protected and unprotected environments, loosing and gaining apparently arbitrarily constitutional protection, and this creating artificial distinctions in an activity that is experienced as uniform by the citizen.

3.4 Article 2.1 Grundgesetz in Conjunction with 1.1 Grundgesetz – The Right to Information Self-determination

Having analysed and rejected as insufficient both Article 10 and Article 13, the Court developed its own answer. It started its analysis by the now commonplace insight that due to recent technological developments, information technology devices are omnipresent in today’s societies and their use is of considerable importance to many citizens.[33] This applies first and foremost to personal computers, but as the Court points out, the relevance of information technology devices is not limited to personal

---

[31] BVerfG, NJW 2008, 822 (843).

[32] M Gercke, “Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit; der Einsatz softwarebasierter Ermittlungsinstrumente zum heimlichen Zugriff auf Computerdaten”, (2007) 23 (4) *Computer und Recht*, 245 (250).

[33] BVerfG, NJW 2008, 822 (841).

computers only. It recognised that many items that are used on an everyday basis by large sections of the German population include elements of information technology.[34] Mobile phones, BlackBerries and even MP3 players are prominent examples for such frequently used devices, intelligent fridges, toasters and even jewellery are already appearing on the horizon as next extensions. Furthermore, the Court recognised that the cultural and social significance of such devices and of personal computers in particular has increased significantly, as they can be used for a large number of different purposes, such as comprehensive administration and archiving of an individual's private and business matters, or in one of the many entertainment applications for leisure activities.[35] Thus the data stored on information technology devices provides comprehensive information about the personal circumstances, social contacts, personal preferences and activities of the user.

The Court argued that for most people, the use of the Internet is an essential part of the way they live their lives, and an important aspect of the way in which they develop and express their personality. It also stated that in addition to the new potential for the development of one's personality, the increasing spread of and reliance on networked information technology devices also creates new dangers for the personal development of individuals. In addition to the potentially sensitive data stored on the devices themselves, the user of a device connected to the Internet will (knowingly and unknowingly) leave data and information related to his personality and user behaviour with intermediaries and on other servers behind. Knowledge about every single piece of such data can be harmless, but, as the Court argued, the combination of the data stored on information technology devices and held by other entities in a network can make it possible to form a profile if a third party collects and evaluates it.[36] Above all, however, the networking of the system opens to third parties a technical access facility, which can be used to spy on or manipulate data kept on the system. The individual cannot detect such access at all in some cases, or at least can only prevent it to a limited degree.[37]

It is the combination of the changing social and cultural significance of the use of information technology devices for the development of one's personality combined with the recognition of new, equally technologically enabled threats to the free development of one's personality through e.g. new data mining capacities, that led the court to recognise the fundamental importance of solidifying constitutional guaranties in online settings.

In the year when the first TCP/IP-based wide-area network was operational and all hosts on the ARPANET were switched over from the older NCP protocols, and five years before the Internet had been opened to commercial providers, the Constitutional Court had in a landmark ruling unrelated to ICT created the core of Germany's data protection law.[38] The right to information self-determination, which is not explicitly mentioned in the constitution, was derived from Article 2.1 in conjunction with Article 1.1 GG, which guarantee the right to free development of one's personality

---

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] BVerfG 65,1.

and a general "right to dignity", respectively. Ruling on the constitutionality of the national census, it establishes a legal entitlement to the capacity of the individual to determine in principle the disclosure and use of one's personal data.[39] This right resulted from the court's recognition that the state had multiple possibilities to collect process and use private data, and that the evolution of electronic data processing techniques had simplified these to such an extent that a detailed image of the personality of the individual became feasible. This had the potential to impair confidentiality interests of the affected person, which are protected by fundamental rights. Moreover, the mere anticipation that one's data could be collected entailed an unacceptable encroachment on one's freedom of conduct, encouraging people to forgo valid, and perfectly legal, lifestyle choices in the mere anticipation that information about them could be collected and leaked to third parties. This means in particular that no concrete threat has to be evident. The Court stated that this is in particular the case if personal data can be used and linked in a manner, which the person concerned can neither detect nor prevent.[40] Fear of surveillance is just as limiting to the free development of a social personality as the surveillance itself.

Both, the *Land* Government of North Rhine-Westphalia and the Federal Government conceded that the right to information self-determination should be a fundamental right standard for online searches, but argued also that it is sufficient to regulate such investigative measures.

However, the Court found that the right to information self-determination does not sufficiently appreciated the fact that individuals rely on information technology systems to develop their personality and hence entrust the system with sensitive data, or inevitably provide such data by merely using the system.[41] A third party accessing such a system can obtain potentially large amounts of sensible information about an individual, without having to rely on further data collection and processing measures. In a way, on could say that these measures cut out the middle man. The data comes already preprocessed and arranged by the data subject. Since the older data protection decision focused on the process of data handling and organization, it was in danger of being circumvented by the new surveillance technology. The active, if unwitting, participation of the suspect that is crucial for the functioning of the RFS had therefore also the potential to deprive the suspect of otherwise taken for granted protection. Online searching of a computer is of a severity for the personality of the affected person that goes beyond mere individual data collection, against which the right to information self-determination provides protection, and is therefore not covered by this fundamental right.

4. The Right in the Confidentiality and Integrity of Information Technology Systems

Having determined that existing rights are not sufficient to protect citizens from the threat against their personality rights, the Court established a new fundamental right

---

[39] BVerfGE 65, 1 (43); 84, 192 (194).

[40] BVerfG, NJW 2008, 822 (844).

[41] Ibid.

in the confidentiality and integrity of information technology systems to close the regulatory gap.

Just like the fundamental right in information self-determination, this right is not explicitly mentioned in the constitution. Although it does not happen very often in Germany that a new basic right is established through judicial activism, the right of the Court to creatively fill identified gaps in the constitution's civil rights framework is widely recognised and, unlike in the US, originalism has never been a prominent position in post-war Germany.[42]

In the same way as the right in information self-determination, this new fundamental right is based on Article 2.1 GG in conjunction with Article 1.1 GG, and is derived from a general personality right. Article 1 GG that states that "Human Dignity is inviolable, and all organs of the state have the ultimate aim to protect it" establishes a general overriding principle in the German legal system, and is designed explicitly as a stop-gap solution if legislative solutions fall behind social change. The new constitutional right in the confidentiality and integrity of information technology systems protects, so the Court, the personal and private life of rights holders from the state accessing information technology devices, and in particular against access by the state of the information technology system as a whole, and not only of individual communication events or stored data.[43]

4.1 Which Systems are protected?

The Court applies the guarantees of this right to information technology systems, but interestingly in doing so does not deliver a definition of such a system. Instead, it lists systems that are not protected by this right, and provides a description of minimum abilities an information technology system must possess to fall into the protection scope of this fundamental right. By doing so, it keeps the protection scope of this basic right very broad and deliberately avoids tailoring this new basic right to specific technologies. It thereby clearly acknowledges the rapid technological developments of information technology devices, and attempts to create technology neutral legislation with this judgement, hence trying to keep the new basic right "future-proof".[44]

The Court finds that not all systems that are able to create, process or store personal data require special protection of a separate guarantee of personal rights.[45] Systems that contain data pertaining to a certain aspect of the affected person's life only are not protected by this new fundamental right. Such systems could, for example, be non-networked electronic control systems in household appliances.[46] Clearly, access to such data would not enable authorities to gain a detailed insight into the personality of the person concerned.

---

[42] R Alexy, R Dreier, "Statutory Interpretation in the Federal Republic of Germany", in N MacCormick and R Summers (eds), *Interpreting Statutes: A Comparative Study* (Darthmouth, Aldershot: 1991) 72-121.

[43] BVerfG, NJW 2008, 822 (846).

[44] See for a discussion on technology neutrality for example, C Reed, "Taking Sides on Technology Neutrality" (2007) 4:3 *SCRIPTed* 263-284.

[45] BVerfG, NJW 2008, 822 (847).

[46] Ibid.

The protective scope of the fundamental right in confidentiality and integrity of information technology system is applied to systems which alone, or in their technical interconnectedness, can contain personal data of the person concerned to such a degree and in such a diversity that access to the system facilitates insight into significant parts of the life of a person or indeed provides a revealing picture of their personality.[47] Such systems are for example personal computers and laptops (used for both private and business purposes), and mobile phones and electronic calendars, which have a large number of functions and can collect and store many kinds of personal data. Interestingly, the Court decided that the mere *ability* of the system to store personal data is sufficient. Whether this capacity was utilised by the user in question need not be determined in the individual case. This means that this right protects a system, such as a computer, even if it does not actually contain sensitive personal data, as long as it is technically able to store and process such information. Furthermore, it acknowledges that systems that are part of a network (such as the Internet) do not always contain personal data themselves, but data about the person concerned can be stored on another system within the network, which however can be accessible if the system is infiltrated. This new fundamental right thus is to apply to data that is outsourced, for example using cloud computing technology.[48] This makes the decision also the first that explicitly recognised the pertinent legal issues that cloud computing and its diffuse ownership and control arrangement will inevitably bring.

4.2 What is protected?

What precisely does the basic right in integrity and confidentiality of information technology systems protect? Firstly, it protects the interest of a user of an information technology system in ensuring that the data created, processed and stored by the system remains confidential.[49] Secondly, this right is violated if the integrity of such a system is affected by the system being accessed in such a way that third parties can use its performance, functions and storage contents. This would mean, as the Court establishes, that the most crucial technical hurdle to enable the spying, surveillance or manipulation of the system would be overcome.[50]

The Court specifies further that this basic right protects the right holder in particular from the clandestine access of an information technology system that is targeted at the system in its entirety or its major parts. The scope of protection of this right covers both the data kept on the working memory as well as data which is temporarily or permanently kept on the storage media of the system. It also protects against data acquisition that does not rely on the data processing procedures of the system itself, but nevertheless targets these, such as so-called key-loggers, which monitor the keystrokes of a user to gain passwords and other crucial login details.[51]

---

[47] Ibid.

[48] For a discussion on Cloud Computing see: M Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law", 6:1 *SCRIPTed* 132-146.

[49] BVerfG, NJW 2008, 822 (847).

[50] Ibid.

[51] Ibid.

The Court further states that the protection arising from this fundamental right does not depend on the degree of difficulty in accessing the system. The Court therefore acknowledges that users of information technology systems have a varying knowledge of technical means to protect systems from being infiltrated by third parties, and does not grant users with a better knowledge a higher degree of protection.

However, a protection only exists if the person concerned considers the system his own, and thus may presume that he alone or others authorised by him, such as close family members, use it in a self-determined manner. Using a public access information technology system in a rail station that provides timetable and travel information is therefore not covered. Covered however is also the use of one's own system via the use of information technology systems that are at the disposal of others. This could, for example, be the remote access of one's system or external storage device via a computer in a cyber café.

4.3 Restrictions

However, the right in the confidentiality and integrity of information technology systems is not absolute. It can be restricted for both preventive purposes and to prosecute crimes. Yet, any measure that restricts this fundamental right has to be proportionate to the violation, especially if the measure is carried out without the knowledge of the suspect. Hence, the Court has found that a measure restricting this right is only proportionate where sufficient evidence exists that significant higher-ranking fundamental values need to be protected. Higher-ranking fundamental values are the life and integrity of other citizens, the foundations of the state, and essential values of humanity.[52] However, the Court then softens this requirement, ruling that a high level of probability that the danger will materialise in the near future is not required.[53]

Furthermore, any such measure has to be scrutinised and confirmed by a judge on a case-by-case basis to guarantee an objective and independent control prior to the execution, and it has to be based on a constitutional legal basis.[54]

A further requirement is that any measure restricting the right in the confidentiality and integrity of information technology systems does not violate the core area of the private conduct of life, which includes among other things communication and information about inner feelings or deep relationships. The private conduct of life is an absolute fundamental right, which cannot be restricted (Article 1.1 GG – right to human dignity). Since it will often be very difficult to differentiate between core area and non-core area data during the investigation process, the Court states that adequate procedures have to be in place for the examination stage of the data. In particular, if core area data is detected, this data has to be deleted immediately and the use of this data by the state is prohibited.[55] However, this raises the dilemma that the requirement to delete the collected core area data cannot undo the violation of the absolute right to

---

[52] BVerfG, NJW 2008, 822 (849).

[53] BVerfG, NJW 2008, 822 (853).

[54] BVerfG, NJW 2008, 822 (854).

[55] Ibid.

human dignity. Furthermore, as Kutscha points out, although the measure itself has to be permitted by a judge, the Court has not established a requirement for a judge to control the analysis process.[56]

5. Conclusion

The reasoning of the Court has been, from a technology or technologically aware perspective, exceptionally well-grounded, thereby gainsaying frequent criticism that legal responses are formed by people ignorant of the relevant technology. Furthermore, the newly developed fundamental right is drafted broadly enough to sufficiently deal with future technological developments.

While the main impetus of the ruling was to increase protection of citizens, the Court has also established that remote online searching of computers is not generally an unconstitutional measure, but that legislation allowing for this will have to be in strict compliance with the right in the confidentiality and integrity of information technology systems *in addition to* the already established protection of Articles 10 GG and 13 GG. One the one hand, this means that the Court has paved the way for Germany to act on the recommendation of the Council of the European Union that Member States should facilitate the clandestine search of computers of suspects to combat cybercrime.[57] At the same time, it has established high procedural hurdles for the use of this technology. An issue that cannot be discussed in this paper is the potential border conflicts that the technology can bring with it, if a RFS migrates on a server outside the jurisdiction of the investigating police, or if a suspects physically carries an "infected" device abroad.[58] Since the protection of Article 1 covers also foreign nationals on German territory, potential for conflict is therefore high if other member states decide to introduce the technology with comparatively lower safeguards

By creating the new fundamental right in the confidentiality and integrity of information technology systems the Court has, for the first time, recognised that information technology not only plays an important role in people's life as an add-on or extension to live in the physical world, but also that an increasing number of people "live" online. The Internet has become a living space, where people make friends, form societies and exchange information, and the Court has acknowledged that existing legislation is insufficient to adequately protect citizens from state violations of this digital environment. The "digital citizen" has, as a result of this case, come a step closer. By the same token, it is not inconceivable that the Court will in the future expand this concept also in the opposite direction. At present, the Federal Trojan is understood as a digital tool used by real, physical police officers. But if the Court

---

[56] See note 5, at 1043.

[57] Council of the European Union, "Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime", 2987th Justice and Home Affairs Council meeting, 27-28 November 2008, at http://www.ue2008.fr/webdav/site/PFUE/shared/import/1127_JAI/Conclusions/JHA_Council_conclusions_Cybercrime_EN.pdf.

[58] See W Abel, "Agents, Trojans and tags: The next generation of investigators", (2009) 23:1&2 *International Review of Law, Computers & Technology* 99-108; and W Abel, B Schafer "Big Browser Manning the Thin Blue Line – Computational Legal Theory Meets Law Enforcement", (2008) 2 *Problema*, 51-84, for a more in-depth analysis of the problems surrounding the remote searching of computers.

takes its own reasoning serious, it could as well consider the Trojan itself as a digital police officer, subject to the same restrictions but also powers that its physical counterparts posses. The future is likely to see new attempts by regional and federal Governments in Germany to create "constitution proof" procedural laws that precede the precise legal foundation required by the Court. We are likely to see challenges against these redrafted laws following suit, giving the Court more opportunity to flesh out the new right into the confidentiality and integrity of information technology systems. In particular the "third party effect" of the ruling has yet to be determined, and the degree in which employers, ISPs and content providers such as Google will also be considered potential infringers of this new right. The UK Phorm saga for instance seems like an ideal application of the new right to private sector actors. This will also require rethinking the precise relation between the new right and its older brother, the right in information self-determination. Information self-determination, as the name expresses, is primarily about the free choice of data subjects, including the choice to share his data. This element of choice is absent from the new right, casting even more doubts if the present practice of data handlers to ask for consent will be sufficient in the future.